#becrypt

Data Protection

Disk Protect : DPE SK

DPE SK is an **uncertified** full disk encryption solution that transparently encrypts data on laptops, desktops, tablets and servers. Derived from Disk Protect Enhanced, it can be purchased and deployed immediately, without external key material.

Support for Windows 10 and touch screen devices.

Background

With over 15 years of experience in developing government approved encryption solutions, Becrypt has designed a product variant more readily available and easy to deploy, without the need for external key material.

DPE SK has been engineered from the same code, by the same people and in the same environment as Disk Protect Enhanced, providing product familiarity and provenance to support today's evolving risk management requirements.

Approval

DPE SK is not a formally approved product, and as such, is not subject to the application processes of government approved variants. Built to enable agility and informed risk management, DPE SK supports the use of evolving hardware platforms at pace.

Keys are self generated (AES 256 bit) using the same algorithms as Disk Protect CPA.

Transparency

DPE SK provides full disk encryption, without any disruption to usability. Once the user has logged in to Windows, DPE SK operates transparently, with the ability for standard applications to be used as normal. Since all data is automatically encrypted, there is no risk that the user can circumvent encryption.

Deployment & Performance

DPE SK has the option to configure a rapid initial encryption wave, significantly reducing initial encryption time from previous Disk Protect Enhanced variants.

All encrypted read/write operations are performed with no noticeable impact on performance.

Pre-boot Authentication

DPE SK supports dual factor authentication with username, password and token.

Authenticating the user at pre-boot allows the software to encrypt the entire hard disk, including the operating system, ensuring that data cannot be accessed using low-level tools.

Features

- Self-keying full disk encryption
- No requirement for external key material
- Pre-boot authentication
- Multi-user support at pre-boot
- Dual factor authentication
- Stand-alone capability

For more information on Becrypt and our solutions, contact us:

info@becrypt.com

0845 838 2080

#becrypt.com

#becrypt

Data Protection

Disk Protect : DPE SK

Specifications

Supported Hardware

> Laptops
> Desktops
> Tablets
> Servers

Boot Method

> BIOS

Supported Disk Format Types

> MBR

Types of Hard Disk Supported

> HDD (spinning)
> SSD

Operating Systems

Desktop;
> Microsoft Windows 10
> Microsoft Windows 8.0 & 8.1
> Microsoft Windows 7

Server;
> Windows Server 2012 R2
> Windows Server 2008 R2

Encryption Algorithm

AES 256 bit

Supported Tokens

> Aladdin eToken Pro 32k, 64k
> Aladdin eToken Java 72k
> SafeNet 5100, 5105 & 5110
> Gemalto .NET v2+, v3
> RSA SID 800 series
> Dallas/Maxim iButton tokens

Existing Data

It is recommended that the hard disk(s) must contain no protectively marked data prior to installation. Initial encryption of the hard drive(s) does not delete existing data, but it is recommended that any existing data is backed up, preferably with a full system backup, prior to installation.

User Authentication

Authentication is by username, strong password and mandatory token. Password policy is set locally.

Multiple Users

A device protected by DPE SK requires one System Administrator who manages user accounts and performs security-sensitive actions. Each device supports up to 31 users.

Purge

The purge feature may be triggered pre-boot or following authentication. Purge destroys essential data, rendering the device unbootable and ensuring that any user data it contains is inaccessible.

Removable Media Encryption

Whilst removable media encryption is not supported, DPE SK may be configured to support hardware encrypted removable devices.

System Recovery

User passwords and tokens are updated or replaced locally by the System Administrator. Full system recovery is performed using recovery data generated during installation.